

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
LYNCHBURG DIVISION

IN THE MATTER OF THE SEARCH OF)
CELLULAR PHONE CURRENTLY)
LOCATED AT THE ATF Roanoke Evidence)
Vault)

Case No. 7:21mj1

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Christopher Burch, a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives, being first duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the cellular device seized from Kevin JETT, further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) under the United States Department of Justice. I have been employed with ATF since January 2020, and I am presently assigned to the Roanoke, Virginia Field Office. I have successfully completed the Criminal Investigators Training Program and Special Agent Basic Training, ATF National Academy, held at the Federal Law Enforcement Training Center in Glynco, Georgia. Prior to this employment, I was employed as a sworn police officer/Trooper for the Virginia State Police for approximately seven years. Prior to that, I was employed as a sworn police officer for the Pittsylvania County Sheriff's Office in Virginia for approximately five years. During those twelve years employed as a sworn police officer in Virginia, I conducted a wide variety of criminal investigations, including narcotic and firearms investigations, and also procured and

executed search and arrest warrants. Since becoming an ATF Special Agent, I have participated in narcotics and firearms investigations involving large conspiracies. I have participated in many searches of residences and businesses of suspected drug traffickers for evidence of criminal activity. This aforementioned experience has given me the knowledge to recognize the methods used by criminal violators and individuals disposed to commit criminal offenses to conceal their overall criminal activities from law enforcement personnel and other persons.

3. During my employment as a law enforcement officer, I have received multiple hours of training in narcotics enforcement and investigative techniques, and I have personally participated in numerous investigations. I have also spoken on numerous occasions with informants, suspects, and other experienced narcotics traffickers concerning the methods and practices of drug traffickers, including the methods and practices used by traffickers of methamphetamine, heroin, and cocaine. I have been involved in the execution of numerous search warrants on electronic devices, including cellphones, and in obtaining location information for those devices.

4. Based on my training and experience investigating narcotics and the distribution of narcotics, I know that it is common for individuals engaged in this activity to use telephonic communications, both cellular (to include voice and text messages) and hard line, to further their criminal activities. I know that “smart” phones play an integral role in the daily lives of individuals engaging in narcotics trafficking and that these individuals use cellular telephones to exchange information with customers and/or source(s) of supply through text messaging, instant messaging, and telephone conversations. I also know that it is common for narcotics trafficker to use multiple “smart” phones to communicate with co-conspirators in order to compartmentalize their illegal activity and avoid detection by law enforcement. Further, I know it is common for

narcotics traffickers to change their phones and phone numbers in order to avoid detection by law enforcement.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. The item to be searched is as follows:
- a. A gray Apple iPhone with clear protective case, stored at the ATF Roanoke evidence vault as Exhibit #6 under case number 768045-20-0026.

STATEMENT OF PROBABLE CAUSE

7. The Lynchburg Police Department (LPD) and ATF have been investigating Kevin Seaton JETT and others for the illegal distribution of controlled substances known as cocaine base. During the investigation numerous controlled purchases of cocaine base were made from JETT whom was subsequently indicted in the Western District of Virginia for a violation of Title 21 U.S.C. § 846 and multiple violations of Title 21 U.S.C. § 841.

8. During the investigation, a LPD confidential reliable informant (CRI) made controlled purchases from JETT and before each purchase a controlled telephone call was made to JETT to confirm the upcoming transaction. Below are a list of dates that controlled purchases and calls were made to JETT:

- a. On November 19, 2019 a controlled phone call was conducted for the purchase of an 8-ball of cocaine.

- b. On November 21, 2019 a controlled phone call was conducted for the purchase of 1 ounce cocaine.
 - c. On November 27, 2019 a controlled phone call was conducted for the purchase of 2 ounces of crack cocaine (cocaine base).
 - d. On December 5, 2019 a controlled phone call was conducted for the purchase of 1 ounce of crack cocaine (cocaine base).
9. During the controlled purchased on November 19, November 27, and December 4, video recorded by the CRI shows JETT working with another individual, Robert Russell Matthews, who is assisting JETT with the preparation and sale of cocaine and crack cocaine.
10. On December 8, 2020, JETT was arrested at his residence 2303 Fort Ave Apt#2 Lynchburg, VA 24501. During the arrest several items of drug related evidence was observed and a search warrant was obtained for the residence. During the search of the residence the cell phone described in the affidavit was located and seized a placed into ATF custody.
11. Based on JETT's criminal activities, your affiant believes a search of JETT's cellular phone will further the criminal investigation. Your affiant knows that drug dealers typically use cellular devices to set up and coordinate drug transactions and other criminal activity, including with co-conspirators. Cellular phones not only provide detailed description of the criminal activities being conducted, but also show the criminal network including other members, locations and activities.
12. JETT's cellular phone is currently in the lawful possession of the ATF and is being stored at the ATF Roanoke evidence vault as Exhibit #6 under case number 768045-20-0026. In my training and experience, I know that the Device has been stored in a manner in

which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the ATF.

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Wireless telephone:* A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. *Digital camera:* A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images.

Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. *Portable media player:* A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. *GPS:* A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. *PDA*: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. *Tablet*: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "Wi-Fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those

functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. *Pager*: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- h. *IP Address*: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. Based on my training, experience, and research, I know that the devices described in Attachment A have capabilities that allow them to serve as a wireless telephone, phone book, digital camera, digital recorder, GPS Navigation, portable media player, and PDA. In my

training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Information contained on the devices including text messages, telephone numbers, email communications, images from the internet, photographs, and video footage are typically stored on the devices and can often be recovered with forensics tools.

- a. There is probable cause to believe that things that were once stored on the cellular telephone may still be recovered for at least the following reasons:
- b. Based on my knowledge, training, and experience, I know that computer files and images or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- d. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- e. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to facilitate narcotics distribution that, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was

used; data that was sent or received; and other records that indicate the nature of the offense.

g.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it contains evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the device described in Attachment A, in order to seek the items described in Attachment B.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

/S/ Christopher Burch

Christopher Burch
Special Agent, ATF

Received by reliable electronic means and sworn and attested to by telephone on this 4th day of January, 2021.

Entered: January 4, 2021

Robert S. Ballou

Robert S. Ballou
United States Magistrate Judge